

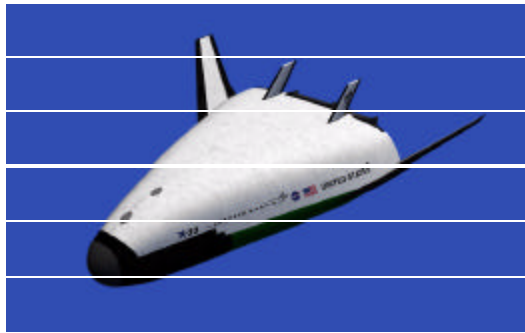
- Excerpt of Full Report -

This document contains excerpts from the X-33 Independent Assessment Report (title page shown below). Only those sections which relate to the PBMA element **Operations** are displayed.

The complete report is available through the PBMA web site, Program Profile tab.

X³³

Safety & Mission Assurance Review



NASA Office of Safety & Mission Assurance

March 5, 1998

2.4 Range/Facilities

The Air Force Flight Test Center (AFFTC) at Edwards Air Force Base (EAFB) has been selected to be the X-33 launch site because proximity to LMSW and the availability of a sparsely populated launch corridor for launches toward the northeast. The X-33 will be launched from the site near Haystack Butte, located at the eastern edge of EAFB. Landing sites include Michael Army Air Field (AAF) at Dugway Proving Ground in Utah and Malmstrom Air Force Base near Great Falls, Montana. The X-33 will be returned to the launch site using a specially designed ground transportation system. Initially the X-33 was to have been ferried back to the launch site via the Shuttle Carrier Aircraft (SCA) now used to ferry the Space Shuttle across country. Approximately 100 workers will construct the \$30 million launch facility, with work scheduled to be completed in a year. Sverdrup Corporation, St. Louis, MO, is overseeing construction of the facility. Site plans include a retractable vehicle shelter; a rotating vehicle launch mount; storage areas for the liquid hydrogen and liquid oxygen propellants, and helium and liquid nitrogen used in vehicle operations; a water storage tank for the sound suppression system; a concrete flame trench; and assorted site infrastructure. The vehicle's operations control center will be located in an existing test control room within Haystack Butte.

2.7 Operations

The X-33 Advanced Technology Demonstrator is an unmanned, autonomous vehicle that uses differential Global Positioning System (GPS) with a radar altimeter for navigation and landing. The differential GPS will guide it through its flight and down the runway for landing. The X-33 will operate as an autonomous vehicle during normal operations. The uplink to the X-33 would only be used if the vehicle deviates significantly from its planned flight path. The X-33 preflight and flight operations will be monitored and controlled from a refurbished operations control center located in Haystack Butte. At the Michael AAF and Malmstrom AFB landing sites there will be a back-up Mobil Operations Control Center only. There will also be range safety officers at the downrange sites. The X-33 is designed to reach Mach 12.6; the current flight test plan specifies a maximum velocity of Mach 12.6 for flight tests to Malmstrom AFB. The X-33 is not designed for, nor intended to, achieve orbital velocities (which would require a speed of more than Mach 25).

2.9 Flight Test Program

No more than 15 flights are currently planned for the X-33 from the EAFB launch site at Haystack Butte. The X-33 Team has defined a series of seven flights that will, if successful, satisfy all program objectives and provide the data needed to establish the confidence for a decision to proceed with the full scale VentureStar. Flights 1-5 will be to Michael AAF and will investigate aero plume and shock-shock interactions, boundary layer transition, thermal protection system (TPS) panel thermal properties, real gas effects, and thrust vector control. Flights 6 and 7 will be to Malmstrom Air Force Base

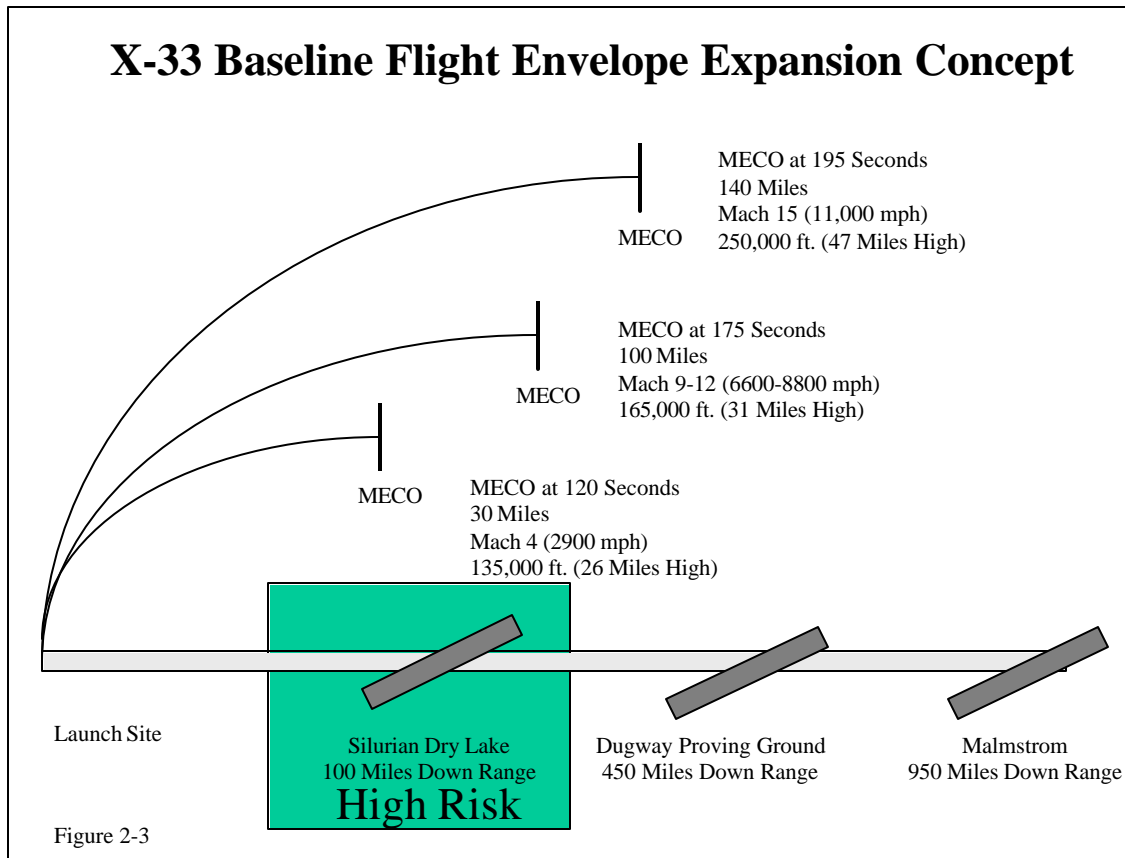
(AFB) and provide additional data on real gas effects. Flights 8 to 15 are to provide additional margin to accommodate test objectives not accomplished in Flights 1-7.

X-33 Flight Test Plan

Test flights involve:

- (1) launching the X-33 from a vertical position like a conventional space launch vehicle - to reduce the structural requirement and weight of the landing gear and wheels to that required to support an unfueled vehicle. The baseline dry weight of the X-33 is approximately 75,000 lb. and fueled weight of is approximately 123,800 kg (273,000 lb);
- (2) accelerating the vehicle to top speeds of Mach 12.6 (12.6 times the speed of sound) or approximately 18,000 km/hr (11,000 mph) and reaching altitudes up to approximately 75,800 m (250,000 ft);
- (3) shutting down the engines and gliding over long distances, up to 1,530 km (950 mi) downrange of the launch site, followed by conducting terminal area energy maneuvers to reduce speed and altitude; and
- (4) landing like a conventional airplane.

The original flight test plan included three short-range, seven mid-range, and five long-range test flights. Using a launch and flight operations site at EAFB, remote landing sites were selected which would accommodate incremental advances to Mach 4, 9, and 15 for the baseline vehicle (Figure 2-3). This would involve flights of approximately 160, 720, or 1,530 km (100, 450, and 950 mi). Actual numbers of test flights to any range would vary due to changing plans and/or actual test flight data evaluation.



Short Range Destination: Silurian Lake, California

(Now eliminated from the flight test program. See discussion under Mission Assurance, Section 5, of this report.)

The U.S. Department of the Interior, Bureau of Land Management (BLM), is the federal government manager of the property and much of the surrounding area. (A pending future action involves transferring this property to the U. S. Army, Ft. Irwin, California, for expansion of their boundaries and capabilities in desert warfare training.) Silurian Lake is classified by BLM as a Multiple Use I (intensive use) area and such activities as commercial filming have been permitted at the site.

Medium Range Destination: Michael Army Air Field on Dugway Proving Ground, Utah

Dugway Proving Ground is located approximately 130 km (80 mi) southwest of Salt Lake City, Utah, near the town of Tooele. Dugway Proving Ground encompasses approximately 324,000 ha (800,000 ac) of the Great Salt Lake Desert. Dugway is part of the U.S. Army Test and Evaluation Command, headquartered at Aberdeen Proving Ground, Maryland.

The airfield within Dugway Proving Ground proposed for landing the X-33 is called Michael Army Air Field. This airfield is located on the eastern boundary of Dugway. The airfield has a 3,960 m (13,000 ft) long by 61 m (200 ft) wide hard surfaced runway.

Immediate surrounding terrain is relatively flat. It is a secure facility with a long history of flight operations. The airspace above Dugway Proving Ground is restricted military airspace controlled by Hill Air Force Base which manages and approves use of the Utah Test and Training Range (UTTR).

Dugway is primarily responsible for planning, conducting, and analyzing tests involving chemical warfare and biological defense systems; flame, incendiary, and smoke obscurant systems; and artillery systems to determine their applicability to military defense programs. The Air Force manages the UTTR at Michael Army Air Field on Dugway. Their primary mission is testing and evaluating unpiloted aerospace vehicles (UAV's) and UAV launch and recovery systems. They support testing of weapons systems; training for operational aircrews and other combat units; maintaining and operating a variety of aircraft; scheduling and monitoring flight activities; and providing range support and air traffic control. UTTR operations are compatible with the mission of the X-33 Program. New site preparation will primarily involve runway lengthening and widening.

Long Range Destination: Malmstrom Air Force Base, Montana

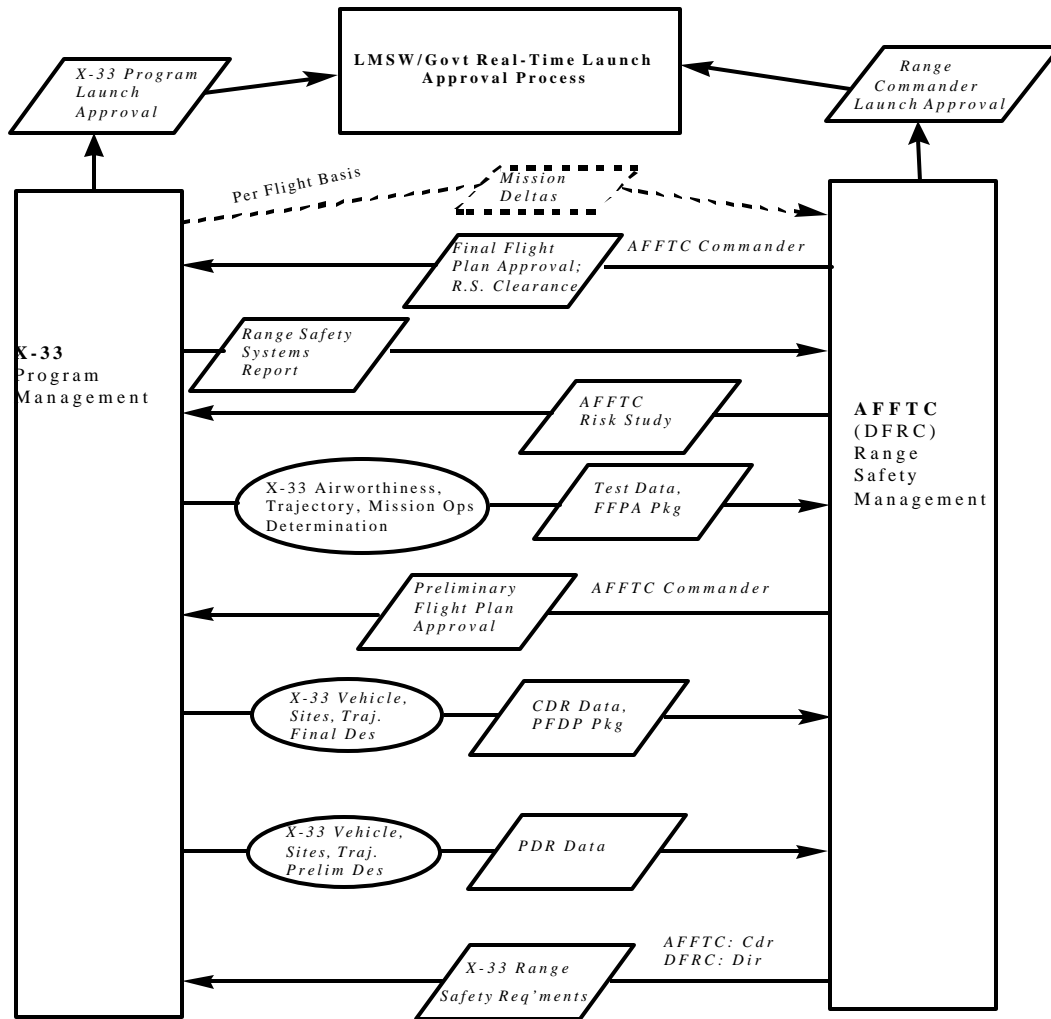
Malmstrom Air Force Base is located 12 km (7 mi) east of downtown Great Falls, Montana. The installation occupies approximately 1,279 ha (3,159 ac). It is home to the 341st Missile Wing (341 MW), which is responsible for operation, maintenance, and security of assigned intercontinental ballistic missile systems. Since the late 1980's, Malmstrom Air Force Base has been home to the 43rd Air Refueling Group. As a result of the Department of Defense's Base Realignment and Closure Plan, the 43rd Air Refueling Group was transferred to MacDill Air Force Base, Florida. After the move, the airfield was closed on December 31, 1996, except for the area used by helicopters of the Malmstrom's Air Rescue Flight. The airfield has a hard surface runway approximately 3,500 m (11,500 ft) long and 61 m (200 ft) wide with a 305 m (1,000 ft) overrun at each end. Since the closure of the airfield, the USAF has no plans or budget to operate the runway. There is no control tower, no instrument landing system, no visual aids for visual approach, no slope indicator lights, no airfield weather support, and no on-going maintenance of the runway. The terrain surrounding the airfield is relatively flat. At the time of the proposed X-33 flights, the airspace will be under Federal Aviation Administration (FAA) control. Reopening of the airfield through permission of the USAF and/or Congressional authorization would be required in order for NASA to land the X-33 at this facility, even on a limited, temporary basis. Discussions with LMSW indicate that this administrative process has been completed.

3.6 Range Safety Process

The Range Safety Process is under the control and direction of the United States Air Force, EAFB Commander. The Range Safety team also works with LMSW Flight Assurance and Operations groups. Flight Assurance chairs the Flight Working Group (FWG), to address issues regarding public safety and emergency preparedness. The Range Safety Office is responsible for all issues regarding Flight Termination System

(FTS) design reliability and redundancy, as well as FTS command-destruct and communication system security. The Range Safety Launch Approval process is mapped in Figure 3.3 shown below.

Figure 3.3 RANGE SAFETY LAUNCH APPROVAL PROCESS



The review team was impressed with the rigorous approach the LMSW/USAF team is using to evaluate and mitigate risks, including coordination with FAA and civil authorities. At the same time, the team acknowledged the need to remain vigilant in examining and discussing risks to public safety and the ways in which these risks will be mitigated. LMSW agreed to provide the review team with the complete Flight Safety Analysis (on CD-ROM), including debris contours, for all phases of flight from Haystack to Dugway and Malmstrom.

X-33 Range Safety Requirements Document (RSRD)

- Excerpt of Full Report -

This document outlines the Range Safety Program and Range Safety requirements for the X-33 flight test program. It defines responsibilities and authorities and delineates policies, processes, and approvals for all range safety activities from design concept through test, checkout, assembly, launch, flight, and landing. This document has been written to primarily address X-33 flight test requirements as they relate to range safety. Specific requirements for system safety, ground safety, launch complex safety, and related matters are not within the scope of this document. These topics are addressed separately by AFFTC, DFRC, and other applicable directives and processes. Table 3-1 sets out risk acceptability guidelines used in development of the RSRD.

TABLE 3-1: Acceptability Guidelines for Pre-launch Launch Area/Launch Complex Hazard Consequences and Probability Categories

HAZARD SEVERITY	POTENTIAL CONSEQUENCES				PROBABILITY*				
Category	Personnel Illness/Injury	Equipment Loss(\$)	Unit Downtime	Data Compromise	A	B	C	D	E
I Catastrophic	May cause death.	> 500,000	> 4 months	Data is never recoverable or primary program objectives are lost.					
II Critical	May cause severe injury or severe occupational illness.	100,000 to 500,000	2 weeks to 4 months	May cause repeat of test program.					
III Marginal	May cause minor injury, or minor occupational illness.	1000 to 100,000	1 day to 2 weeks	May cause repeat of test period.					
IV Negligible	Will not result in injury, or occupational illness.	< 1000	< 1 day	May cause repeat of data point, or data may require minor manipulation or computer rerun.					

RISK PRIORITY:  Unacceptable  Waiver or deviation required  Operation permissible

* Refers to the probability that the potential consequence will occur in the life cycle of the system (test/activity/operation). Use the following list to determine the appropriate Risk Level.

	DESCRIPTION**	THRESHOLD LEVEL	PROBABILITY VALUE	SPECIFIC INDIVIDUAL ITEM	FLEET OR INVENTORY***
A	Frequent	8X10 ⁻²	3X10 ⁻¹	Likely to occur repeatedly	Continuously experienced
B	Reasonably probable		3X10 ⁻²	Likely to occur several times	Will occur frequently
C	Occasional	8X10 ⁻³	3X10 ⁻³	Likely to occur sometime	Will occur several times
D	Remote		3X10 ⁻⁴	Unlikely to occur, but possible	Unlikely, but can reasonably be expected to occur
E	Extremely improbable	8X10 ⁻⁵	3X10 ⁻⁵	The probability of occurrence cannot be distinguished from zero	Unlikely to occur, but possible

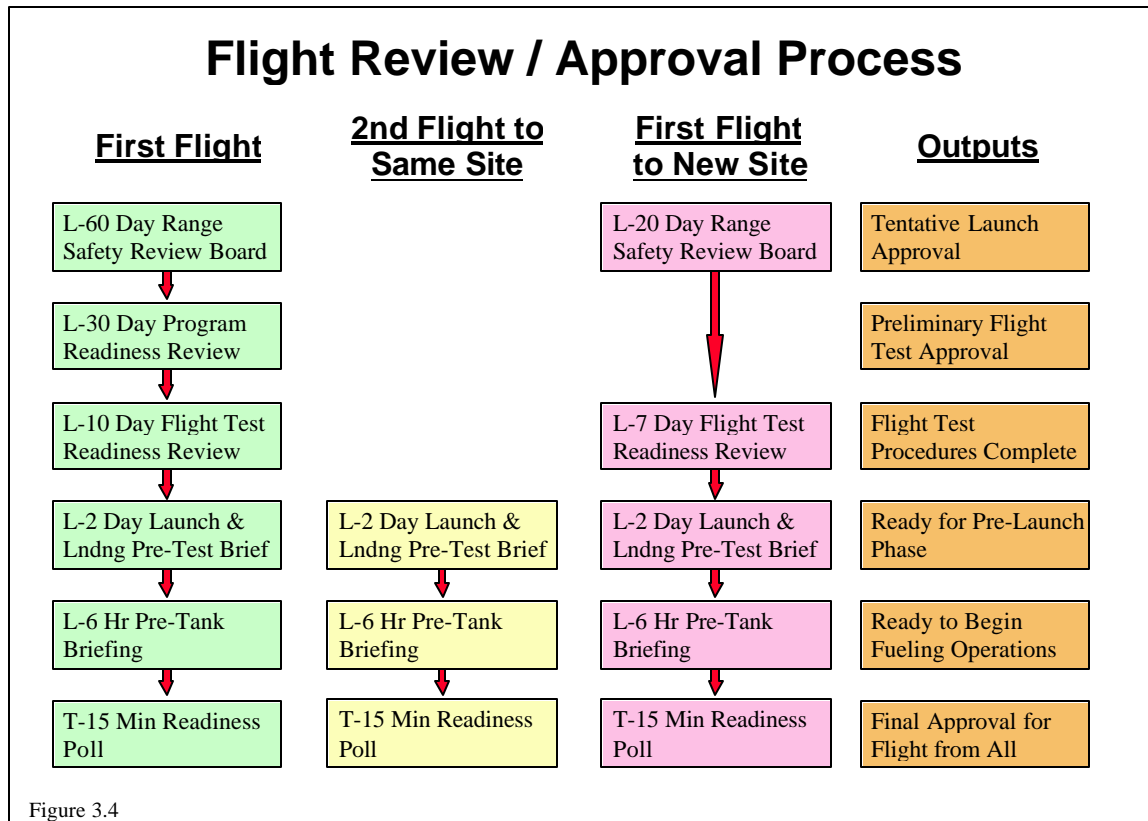
** Definitions of descriptive words may have to be modified based on quantity involved.

*** The size of the fleet or inventory and system life cycle should be defined.

Independent Review Teams (IRT)

Independent review teams comprised of individuals who are knowledgeable and who have no vested interest or decision-making role will participate in all critical program pre-launch milestone reviews, such as L-60 day and L-30 day safety and readiness reviews. The Range Safety IRT is co-chaired by the AFFTC-Range Safety Office with

support from the NASA/DFRC Operations Office. This IRT provides information to the commander for his final decision to allow the X-33 to launch. Figure 3-4 provides an outline of planned operational reviews.



4.0 Safety of Flight Issues

Worst case scenarios for risk exposure are associated with either; 1) a catastrophic, in-flight failure event, explosion, or breakup of the vehicle, or 2) initiation of the FTS in response to anomalous flight trajectory.

The metric employed in range safety analysis is the Expected Casualty (Ec) probability. The range safety criteria is 30 in 1 million (30×10^{-6}). Scenario 1 has a higher probability of causing casualties than Scenario 2 because of the extent of the debris created in a catastrophic event (estimated at over 1000 individual pieces of debris). Scenario 2 assumes a ballistic trajectory of an intact vehicle, initiated by the FTS involving "hard over" commands to both body control surfaces. Safety of flight analyses utilize Scenario 1 (worst case) to bound the maximum expected casualty event. The Ec value for Scenario 1 is 5.0×10^{-6} for flight to Michael Army Air Field in Utah and 5.5×10^{-6} for flight to Malmstrom Air Force Base in Montana. Both estimates meet the range safety criteria of 30×10^{-6} for Ec.

4.1 Powered Flight On-Trajectory Explosion Failures

The X-33 Environmental Impact Statement (EIS) used a projected failure rate of $1/250$, “derived from 220 seconds of powered flight” from consideration of the flight records of Atlas, Delta, Titan II, and Space Shuttle LOX-LH2 engines. The EIS used a projected failure probability of $1/6823$ for non-powered (or coast) flight. This estimate is based on engineering reliability analysis of component failure data and degree of redundancy.

While vehicle reliability is a central Mission Assurance issue, the ultimate public safety risk mitigator is the Flight Termination System (FTS) which is designed to bring the vehicle down intact within the range safety limits.

4.2 Flight Termination System (FTS)

FTS Overview

Command Receiver Decoder (CRD) receives signal, decodes signal, and initiates termination function. Ground-based Command Transmitter System (CTS) generates, modulates, and transmits the signal. Differences between secure and non-secure systems involve; 1) destruct command generation in the CTS, and 2) decoding of the destruct command on-board the vehicle. The IG indicated that a cost increase on the order of \$85K to \$120K would be associated with implementation of secure system hardware. Additional costs would be associated with program compliance with security control and handling requirements.

Failure to Secure Control of FTS Command Uplink

The NASA Inspector General (IG) has recommended implementation of a high security FTS command/destruct decoder-initiator system and an equally secure command uplink system. Tampering, spoofing or other intentional interference with the FTS could result in destruction of the vehicle during nominal operation or impairment of range safety’s ability to terminate flight in the case of an errant ground track. FTS security issues and the perceived need for special security measures are under the authority of the EAFB Commander and Range Safety officials. In discussions with both the IG investigators (at NASA Headquarters) and the Range Safety officials, during the on-site review, it became apparent that a fundamental difference of opinion exists concerning the existence of a credible security threat to operations on the California/Utah/Montana test range.

Resolution

The review team and the X-33 team mutually acknowledged that additional mitigation measures (i.e., secure FTS system deployment) would be appropriate if a credible threat was present. The NASA SMA team took the action to facilitate direct communication between the IG team and the EAFB Range Safety Director to resolve the issue.

4.3 FTS Failure Modes/Reliability

The program is designed to contain Ec well below the required 30×10^{-6} . The current estimate is on the order of 5 or 6×10^{-6} . If the FTS fails to operate properly, the risk management process will have failed and risk exposure will be unlimited, as is the case with the Space Shuttle, Titan IV and other similar space flight launch systems. The FTS reliability and failure modes must be carefully evaluated and risk mitigation strategies verified. It is understood that the Range Safety Independent Review Team (IRT) will provide a measure of verification. However, the review team believes that it would be appropriate for NASA SMA to closely monitor this activity.

4.4 FTS Redundancy

It was noted that the Utah Test and Training Range (Dugway Proving Grounds) personnel do not believe that the current X-33 FTS configuration is fully redundant. This is an open issue that needs follow-up. The review team acknowledged the importance of attaining a full understanding of FTS reliability, failure modes, and failure mitigation.

4.5 Other Information Security Issues

In response to another IG recommendation, the LMSW indicated that they are implementing a program-wide information security analysis and risk mitigation activity.

Appendix B

Aerospace Safety Advisory Panel Report

Memorandum

To: ASAP Members and Consultants

From: ASAP X-33 Group - Richard Blomberg, Ken Englar, George Gleghorn,
Norris Krone, Roger Schaufele

Subject: X-33 Safety Review - 18-19 February 1998 at Palmdale, CA

General

The Aerospace Safety Advisory Panel was invited to attend a Code Q safety review of the X-33 flight test program that was held at the Lockheed Martin "Skunk Work's" Palmdale facility on February 18-19, 1998. In attendance were the ASAP members (as shown above), representatives of Marshall (MSFC), Dryden (DFRC), the Air Force Flight Test Center (AFFTC), the FAA and the Lockheed Martin Skunk Works Corporation (LMSW).

The meeting commenced with a statement of the primary meeting objective by Fred Gregory, which simply stated was to gain a complete understanding of the X-33 program office's safety related risk management and mission assurance process.

The Code Q staff with cooperation of the Dryden Flight Research Center's X-33 flight test manager, developed an excellent agenda for the review which included an extremely comprehensive set of questions ranging from the status of the risk management plan to the methods of documenting and communicating risk information throughout the X-33 project.

Officially the overall management of the program is the responsibility of Lockheed Martin with the NASA Centers acting as "subcontractors" in a government/industry partnership; however, since the final launch authority rests with the government and the government is furnishing approximately 80% of the funding for the program. It is therefore clear that NASA has a significant responsibility to oversee the program. In this regard, MSFC is the designated Lead Center with its functions specified by the NASA Strategic Management Handbook as modified for the special government/industry partnership of the X-33 program. A small MSFC program office is located at the Lockheed Martin Palmdale facility. The office does not presently have a full time S&MA representative, but an agreement was reached at the meeting to add one from MSFC. A Memorandum of Agreement, as yet unsigned, between MSFC and DFRC defines the responsibility of DFRC regarding system safety, range safety, software assurance and, to a limited extent, quality assurance. The NASA Langley Research Center also has a role to perform independent assessments of the concept design, conduct life cycle costs and tradeoff studies, and evaluate the technology benefits to be gained by the X-33 program. It was abundantly clear that Lockheed Martin has a great desire to cooperate and share with the government the responsibility for all safety related aspects

of the program. The briefings presented by Lockheed Martin were comprehensive, meaningful and well presented.

The X-33 Vehicle and Flight Program

The X-33 flight program is one element of Phase II of the larger Reusable Launch Vehicle (RLV) effort. The decision to proceed with Phase III - a full-scale operational RLV vehicle – will primarily depend upon the knowledge gained from and success of the X-33 flight tests. Accordingly, the stated goals of the X-33 are: (1) mature the technologies necessary to design and build a single stage to orbit RLV system, (2) assess the ability to operate the system in a rapid turnaround, low-cost (relative to the space shuttle) mode, and (3) reduce the risks for future RLV private investors. The vehicle is fundamentally an uninhabited flying rocket propulsion system that includes the revolutionary “linear aerospike” engine, internal hydrogen and oxygen tanks, flight and propulsion control systems, the command and control vehicle systems (including the flight termination system-FTS), an autonomous INS/GPS navigation and precision landing system, and the landing gear.

The flight test plan calls for a total of 15 flights of a single vehicle. The first five flights will terminate at Michael Army Air Field (at Dugway Proving Grounds in Nevada), and the remaining flights will end at Malmstrom AFB (Montana). It was briefed that the first seven flights would be sufficient to attain all of the program objectives if all seven were completely successful. Since this is highly unlikely, there are eight additional flights included in the flight plan. The basic approach is that when the flight test objectives are all achieved, the flights will stop. There is no particular necessity to complete any specific number of flights past the first seven.

The launch site is on the Edwards AFB range at the Haystack Butte Launch Site. The X-33 launch facility is being constructed as part of the program. Since neither Dryden nor Edwards are experienced in vertical rocket launches, personnel from Kennedy and Vandenberg are supporting the X-33 program.

The flight profiles for the tests will initially be through the Air Force Flight Tests Center (AFFTC) test range followed by transits through well established military corridors (sparsely inhabited) that have been used previously by the military for cruise missile tests. The overall responsibility for test safety and public safety lies with the Commander of the AFFTC. The AFFTC and DFRC jointly authored an X-33 Range Safety Requirements Document which by coincidence was delivered to LMSW on February 19, the day of this review. Also, the first part of the Preliminary Flight Data Package was delivered by LMSW with the remainder due on the 28th of the month. The AFFTC Range Safety reply to the data package is due in six months. The data will be used by AFFTC to establish whether or not the flight tests planned will result in probable danger to the public that exceeds reasonable limits. The goal is to have no greater danger than provided by normal day-to-day overflights of civil aircraft.

It is apparent that the program is pursuing a major risk management program that is capable of identifying, characterizing, and mitigating any significant safety risks inherent in the X-33 flights. One significant motivation for reducing the flight risks by all means possible emanates from the decision to build only one vehicle. With the potential to lose over a billion dollars resting on the single vehicle, the large effort being planned for testing, software verification, simulation and comprehensive risk analysis is well justified.

Potential Safety Issues

The X-33 program has an excellent risk mitigation, and failure effects and modes analysis plan. The primary threat to human safety is the loss of control of the vehicle (at any time between the launch and the wheels landing at the recovery site) with a resultant striking of the ground in an inhabited area. The impact area could be large if the vehicle broke into a large number of parts or small if the vehicle remained essentially intact. There were a number of areas that the ASAP group felt were potential safety issues and that were in need of future evaluation and explanation. Posed as questions, these areas are:

1. To achieve its trajectory, the vehicle must be programmed so that its instantaneous impact point (the point where the vehicle would impact the Earth's surface if its thrust were to be instantly terminated) crosses territory outside the Air Force Test range while there is still a substantial amount of propellant remaining. Specifically, it must cross a corridor containing US Highway 395 and California State Highway 53 when about half-way through powered flight. Is there a safety analysis of the potential hazard when flight termination occurs prior to propellant exhaustion(MECO)?
2. The flight termination system on the X-33 merely delivers hard-over surface commands to tumble the vehicle, but does not necessarily destroy the vehicle. This is contrary to current vertical launch rocket vehicles. It leaves open a whole slew of concerns about where does this flying "rock" go, particularly if it has flight control surfaces that are stuck in some position that may still cause the vehicle to fly in some unpredicted, or attitude control thrusters that are bleeding down the propellant tanks to produce a similar unpredictable trajectory. The prediction of IIP for X-33 is more complicated than for a normal rocket launch vehicle. During flight through the corridors to the destination where high mach numbers are attained, what is the IIP and the probability of causing injury or death to individuals on the ground or in aircraft?
3. What are the assurances that the communication links with the vehicle will be effective in the event that range safety officers need to assert control over the vehicle?
4. What are the assurances that there will be no inadvertent impact with the chemical/biological weapons material stored at Dugway located near Michael AAF?
5. Is the Flight Termination System (FTS) adequate to assure fool-proof operation if needed? Is the communication for the FTS activation totally redundant? In the event of a flight control failure, is it possible that the FTS would be unable to tumble the vehicle to cause vehicle destruction?
6. Is there a possibility of confusion or procedural error in the hand-off between the primary operations control center and the moveable operations control center? How

does the system design reduce the risk of conflicting inputs or ambiguity in the command authority? Likewise, how will potentially competing inputs be handled when downmoding after an early MECO?

7. What procedures are being employed to assure a secure communications link that has no credible threat of sabotage? Are the communication links planned as secure as the ones used on the Air Force cruise missiles that fly the routes to be used by the X-33? Alternatively, is it definite that a communications compromise with a malicious intent cannot command the vehicle in a way that would compromise safety?
8. How extensive are simulation activities in emulating the actual flight conditions and determining effects of potential mishaps?
9. What is the system safety plan regarding the launch site procedures?

Summary

The obviously strong interaction among the Air Force range safety people, NASA Dryden personnel and the X-33 project (MSFC and LMSW) indicates that significant checks and balances are inherent in the process of developing and approving flight test plans. This should lead to the appropriate identification and mitigation of risks.

The risk management process that was summarized in the briefing by the project appears suitable and capable of identifying, characterizing and mitigating any significant safety risks inherent in the X-33 tests. There was no evidence of shortcuts being taken or any attempts to circumvent prudent safety approaches. As long as the project remains committed to the approaches outlined at the briefing, it should be capable of managing risk to the lowest possible level for an autonomous rocket vehicle with significant technological advances.

Implications for Future ASAP Activities

Since the vehicle is unmanned and there appears to be adequate attention being paid to safety issues, there is no need for a large ASAP involvement in the X-33 Program. However, the Panel should monitor the program activities to understand any safety-related decisions and to be aware of decisions that might impact the design of the future RLV vehicle that is planned to carry humans.

cc: Fred Gregory